

PATENT OFFICE
JAPANESE GOVERNMENT



This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: October 19, 1999

Application Number: Patent Application
 No. 11-296669

Applicant(s): CASIO COMPUTER CO., LTD.

April 7, 2000

Commissioner,
Patent Office Takahiko Kondo

Certificate No. 2000-3024160

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

JC925 U.S. PT.
09/670424
09/26/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出 願 年 月 日
Date of Application:

1999年10月19日

出 願 番 号
Application Number:

平成11年特許願第296669号

出 願 人
Applicant(s):

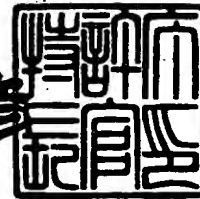
カシオ計算機株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 4月 7日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3024160

【書類名】 特許願

【整理番号】 A009906035

【提出日】 平成11年10月19日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 12/00
G09C 1/00

【発明の名称】 データベース管理装置、データベースシステム及び記録媒体

【請求項の数】 6

【発明者】

 【住所又は居所】 東京都羽村市栄町3丁目2番1号 カシオ計算機株式会社羽村技術センター内

 【氏名】 森 潤二

【発明者】

 【住所又は居所】 東京都渋谷区本町1丁目6番2号 カシオ計算機株式会社内

 【氏名】 黒澤 和大

【特許出願人】

 【識別番号】 000001443

 【氏名又は名称】 カシオ計算機株式会社

【代理人】

 【識別番号】 100058479

 【弁理士】

 【氏名又は名称】 鈴江 武彦

 【電話番号】 03-3502-3181

【選任した代理人】

 【識別番号】 100084618

 【弁理士】

 【氏名又は名称】 村松 貞男

【選任した代理人】

【識別番号】 100068814

【弁理士】

【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9005919

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データベース管理装置、データベースシステム及び記録媒体

【特許請求の範囲】

【請求項 1】 データベースの所定の列項目のデータについて当該列項目に共通の列鍵を用いて暗号化し、その他の列項目のデータについては各行毎に固有の行鍵を用いて暗号化する第 1 の暗号化手段と、

この第 1 の暗号化手段による前記データベースの他の列項目のデータの暗号化に用いられた行鍵を各行に共通の別の鍵を用いて暗号化する第 2 の暗号化手段と、

前記第 1 の暗号化手段によって暗号化されたデータベースを前記第 2 の暗号化手段によって暗号化された行鍵と共に記憶する記憶手段と

を具備したことを特徴とするデータベース管理装置。

【請求項 2】 前記行鍵は、前記データベースの各行に割り当てられた行番号と乱数とによって生成されることを特徴とする請求項 1 記載のデータベース管理装置。

【請求項 3】 データベースを管理する第 1 の端末装置と、この第 1 の端末装置とは独立して前記データベースの検索を行う第 2 の端末装置とで構成されたデータベースシステムであって、

前記第 1 の端末装置側で、前記データベースを暗号化し、その暗号化データベースを可搬型の記録媒体に記録して配布し、

前記第 2 の端末装置側で、前記配布された記録媒体を用いて、そこに記録された暗号化データベースに対するデータ検索を行い、その検索結果として得られたデータを復号化して表示することを特徴とするデータベースシステム。

【請求項 4】 前記第 1 の端末装置は、

前記データベースの所定の列項目のデータについて当該列項目に共通の列鍵を用いて暗号化し、その他の列項目のデータについては各行毎に固有の行鍵を用いて暗号化すると共に、前記行鍵を各行に共通の別の鍵を用いて暗号化し、

この暗号化されたデータベースを前記暗号化後の行鍵と共に記録媒体に格納す

ることを特徴とする請求項 3 記載のデータベースシステム。

【請求項 5】 前記記録媒体には、前記第 1 の端末装置にて暗号化されたデータベースと共にその暗号化データベースを検索するための所定のプログラムが格納されることを特徴とする請求項 3 記載のデータベースシステム。

【請求項 6】 コンピュータに、

データベースの所定の列項目のデータについて当該列項目に共通の列鍵を用いて暗号化し、その他の列項目のデータについては各行毎に固有の行鍵を用いて暗号化する第 1 の暗号化機能と、

この第 1 の暗号化機能による前記データベースの他の列項目のデータの暗号化に用いられた行鍵を各行に共通の別の鍵を用いて暗号化する第 2 の暗号化機能と
を実行させるためのプログラムを記録したコンピュータ読取り可能な記録媒体

。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、データベースを暗号化して管理するデータベース管理装置、データベースを提供する端末とデータベース検索を行う端末とからなるデータベースシステム及びデータベースを暗号化するためのプログラムを記録した記録媒体に関する。

【0002】

【従来の技術】

データベース管理装置では、データベースのセキュリティを確保するため、管理対象として保有しているデータベースを暗号化して保存しておくことが求められる。

【0003】

ここで、データベースを暗号化する場合に、例えばパスワード等によって生成された 1 つの固定的な暗号化鍵を用いて対象ファイル全体を暗号化するのが一般的であった。

【0004】

【発明が解決しようとする課題】

データベースは膨大なデータ量を有し、その中には機密性の高いデータ項目も含まれており、他のデータ項目よりもセキュリティを高くすることが要求される。しかしながら、上述したように従来方式では、1つの固定的な暗号化鍵を用いて暗号化していたため、各データ項目のセキュリティレベルは同じになり、しかも、同じデータを持つ項目があった場合には暗号化結果も同じになってしまい、そこから暗号化鍵が解読される危険性があった。

【0005】

本発明は前記のような課題を解決するためになされたもので、データベース上の特定のデータ項目に対するセキュリティを他のデータ項目よりも高めて暗号化することのできるデータベース管理装置、データベースシステム及び記録媒体を提供することを目的とする。

【0006】

【課題を解決するための手段】

本発明は、データベースを暗号化する際に、検索に利用される列項目のデータについては当該列項目に共通の列鍵を用いて暗号化し、その他の列項目のデータについては高セキュリティが要求される項目として各行毎に固有の行鍵を用いて暗号化し、さらに前記行鍵を各行に共通の別の鍵を用いて暗号化するようにしたものである。

【0007】

具体的には、本発明のデータベース管理装置は、データベースの所定の列項目のデータについて当該列項目に共通の列鍵を用いて暗号化し、その他の列項目のデータについては各行毎に固有の行鍵を用いて暗号化する第1の暗号化手段と、この第1の暗号化手段による前記データベースの他の列項目のデータの暗号化に用いられた行鍵を各行に共通の別の鍵を用いて暗号化する第2の暗号化手段と、前記第1の暗号化手段によって暗号化されたデータベースを前記第2の暗号化手段によって暗号化された行鍵と共に記憶する記憶手段とで構成される。

【0008】

このような構成によれば、データベースを暗号化する際に、検索に利用される

所定の列項目以外の列項目のデータについては、各行毎に鍵を異ならせて暗号化することで、その列項目の中に同じ値のデータがあっても、異なる値として暗号化結果を得ることができ、しかも、当該列項目の暗号化に用いられた鍵（行鍵）を別の鍵で再暗号化することで、鍵の解読を困難として高セキュリティ化を実現できる。

【0009】

また、前記データベースの各行に割り当てられた行番号と乱数とによって前記行鍵を生成するようにすれば、鍵の解読がさらに困難となり、セキュリティを強化することができる。

【0010】

また、データベースを管理する第1の端末装置と、この第1の端末装置とは独立して前記データベースの検索を行う第2の端末装置とでデータベースシステムを構築することも可能である。

【0011】

このデータベースシステムでは、第1の端末装置側にて前記データベースを暗号化し、その暗号化データベースを記録媒体に記録して配布し、第2の端末装置側にて前記配布された記録媒体を用いて、そこに記録された暗号化データベースに対するデータ検索を行い、その検索結果として得られたデータを復号化して表示する。この場合、前記のようにデータベースの所定の列項目のデータについて当該列項目に共通の列鍵を用いて暗号化し、その他の列項目のデータについては各行毎に固有の行鍵を用いて暗号化すると共に、前記行鍵を各行に共通の別の鍵を用いて暗号化することで、記録媒体にデータベースを格納して配布したとしても、そのセキュリティを確保することができる。

【0012】

【発明の実施の形態】

以下、図面を参照して本発明の実施形態を説明する。

【0013】

（第1の実施形態）

図1は本発明の第1の実施形態に係るデータベース管理装置の構成を示す図で

ある。本装置は、行と列からなるマトリクス形式のデータベースを暗号化して管理する機能と共に、その暗号化されたデータベースを検索する機能を備えたものであって、例えば磁気ディスク等の記録媒体に記録されたプログラムを読み込み、このプログラムによって動作が制御されるコンピュータによって実現される。

【0014】

図1に示すように、本装置には、CPU 11、表示装置12、入力装置13、プログラム記憶装置14、鍵生成装置15、データ記憶装置16、データベースI/F 17が設けられている。

【0015】

CPU 11は、本装置全体の制御を行うものであり、プログラム記憶装置14に記憶されたプログラムを読み込み、そのプログラムに従って各種処理を実行する。本実施形態において、CPU 11は図8に示すようなデータベースの暗号化処理や、図9及び図10に示すようなデータベースの検索処理を実行する。

【0016】

表示装置12は、データを表示するためのデバイスであり、例えばLCD (Liquid Crystal Display) やCRT (Cathode-ray tube) 等が用いられる。入力装置13は、データを入力するためのデバイスであり、例えばキーボード、マウス等が用いられる。

【0017】

プログラム記憶装置14は、例えばROMあるいはRAMなどで構成され、本装置に必要なプログラムを記憶する。本装置に必要なプログラムとしては、データベース暗号化プログラムやデータベース検索プログラム等がある。

【0018】

なお、プログラム記憶装置14は半導体メモリの他に磁氣的、光学的記録媒体で構成することができる。この記録媒体はCD-ROM等の可搬型の媒体やハードディスク等の固定的な媒体を含む。また、この記録媒体に格納するプログラムは、その一部若しくは全部をサーバやクライアントからネットワーク回線などの伝送媒体を介して伝送制御部から受信する構成にしてもよく、更に、前記記録媒体はネットワーク上に構築されたサーバの記録媒体であってもよい。更に、前記

プログラムをネットワーク回線などの伝送媒体を介してサーバーやクライアントへ伝送してこれらの機器にインストールするように構成してもよい。

【0019】

鍵生成装置 15 は、データベースの暗号化に用いられる暗号化鍵を生成するためのデバイスであり、ここでは暗号化鍵として基本鍵、行鍵、列鍵の 3 つの鍵を生成するための基本鍵生成部 15 a、行鍵生成部 15 b、列鍵生成部 15 c から構成されている。

【0020】

データ記憶装置 16 は、本装置に必要な各種のデータやテーブルを記憶するためのデバイスであり、例えば RAM あるいは磁気ディスク装置等の外部記憶装置で構成される。このデータ記憶装置 16 には、基本鍵パラメータテーブル 16 a、基本鍵記憶部 16 b、鍵スペックテーブル 16 c、暗号化データ格納部 16 d、検索文字列格納部 16 e が設けられている。

【0021】

基本鍵パラメータテーブル 16 a は、基本鍵のパラメータ値が登録されたテーブルである（図 4 参照）。基本鍵記憶部 16 b は、オペレータの指定操作によって得られた基本鍵のパラメータ値を記憶する。鍵スペックテーブル 16 c は、データベースの各列（フィールド）毎に定義された暗号化方式の種類（非暗号化、行鍵、列鍵）を記憶するテーブルである（図 6 参照）。暗号化データ格納部 16 d は、暗号化されたデータベースを格納する。検索文字列格納部 16 e は、データベース検索時にオペレータにより指定された検索用文字列を格納する。

【0022】

データベース I/F 17 は、本装置とは独立して設けられた外部データベース記憶装置 18 との間でデータの授受を行うためのインタフェースである。この外部データベース記憶装置 18 は、複数のデータベースファイル（オリジナルデータ）を有しており、これらのデータベースファイルは本装置からのアクセスによって選択的に読み出されるように構成されている。

【0023】

ここで、本装置の動作を説明する前に、理解を容易にするため、本装置におけ

るデータベースの暗号化方法について説明しておく。

【0024】

データベースを暗号化する場合に、各行毎（レコード毎）に異なる鍵を用いて暗号化すれば鍵の解読は困難となり、セキュリティ性を高めることができる。しかし、すべての行について鍵を異ならせると、データベースを検索する際に、暗号化されているデータを各行毎の鍵で復号化するか、または、検索用として入力されたデータ（キーワード）を各行毎の鍵で暗号化しなければならいため、検索結果を得るのに時間がかかることになる。一方、各列毎（フィールド毎）に異なる鍵を用いてデータベースを暗号化すると、検索対象となる列項目に対応した鍵のみを用いて検索用データを暗号化すれば良いのでデータベース検索を高速に行うことができる。しかし、同じ列の中で同一のデータがあると、暗号化結果も同じになってしまうため、そこから鍵を解読される可能性が高くなる。

【0025】

そこで、本発明では、データベースを暗号化する際に、検索に頻繁に利用される列項目のデータについては非暗号化あるいはその列項目に共通の鍵（列鍵）で暗号化し、その他の列項目のデータについては高セキュリティが要求される項目として、各行毎に異なる鍵（行鍵）で暗号化し、さらに、各行毎に異なる鍵（行鍵）を各行に共通の別の鍵（基本鍵）で再暗号化することを特徴とする。つまり、高セキュリティが要求される列項目のデータについては、各行毎に暗号化鍵を異ならせ、さらに、その暗号化鍵をシステム基本鍵で暗号化することで、高セキュリティ化を実現するものである。

【0026】

図11に具体例を示す。

【0027】

図11は本装置によるデータベースの構成を説明するための図であり、図11（a）は暗号化前の状態、同図（b）は暗号化後の状態、同図（c）は復号化後の状態を示している。

【0028】

図11（a）に示すように、本装置では、行と列からなるマトリックス形式の

データベースを暗号化対象としている。ここでは、個人データをデータベース化したものを示している。このデータベースには、「code」、「name」、「state」、「age」、「phone」の各列項目（フィールド）を有する。

【0029】

このようなデータベースに対し、列鍵と行鍵を用いて暗号化を行う。すなわち、検索に頻繁に利用される列項目を「state」、「age」とした場合に、これらの列項目の各行のデータ（レコード）については、各列項目に共通の列鍵を用いて暗号化し、その他の列項目「name」、「phone」の各行のデータ（レコード）については高セキュリティが要求される項目として、各行毎に固有の行鍵を用いて暗号化してレコードファイルに格納する。その際に、当該列項目の暗号化に用いられた行鍵を基本鍵で再暗号化し、その暗号化された行鍵を各レコードに付加して格納する。なお、「code」の列項目のデータについては暗号化を行わないものとする。

【0030】

図11（a）のデータベースを列鍵と行鍵を用いて暗号化した結果を図11（b）に示す。この場合、「line key」といった列項目が追加され、そこに基本鍵で暗号化された行鍵（9658, 9143, 8278…）が格納される。図1に示すデータ記憶装置16の暗号化データ格納部16dには、図11（b）に示すような状態でデータベースが保存されることになる。

【0031】

また、データベースを検索する場合には、検索に利用される列項目に対応した列鍵を用いて検索用データを暗号化してから検索処理を行う。例えば、「state」の中の「Florida」といったデータを検索する場合には、まず、検索用データとして入力された「Florida」を「state」の列鍵で暗号化して、「h*/fDD」を得る。この「h*/fDD」といったデータを「state」の列の各行から検索する。これにより、「code2」と「code8」に該当するデータが存在することがわかる。

【0032】

また、暗号化されたデータベースを元に戻す場合には、暗号化の時と同じ列鍵、行鍵、基本鍵を用いる。図 1 1 (b) のデータベースを暗号化の時と同じ列鍵、行鍵、基本鍵を用いて復号化すると、図 1 1 (c) に示すように元のデータを得ることができる。

【0033】

次に、このようなデータベースの暗号化／復号化を実現するための具体的な構成について説明する。

【0034】

図 2 は本装置の構成を機能的に示したブロック図である。

【0035】

本装置を機能的に示すと、入力処理系は基本鍵指定部 2 1、基本鍵設定部 2 2、鍵スペック入力部 2 3、鍵スペック設定部 2 4 で構成される。また、暗号化処理系はデータ読出し部 2 5、レコード入力メモリ 2 6、暗号化処理部 2 7、暗号化レコード書込メモリ 2 8、データ書込み部 2 9 で構成され、復号化処理系は暗号化レコード読出メモリ 3 0、復号化処理部 3 1、レコード出力メモリ 3 2、データ出力部 3 3 で構成される。また、この他に、上述した基本鍵パラメータテーブル 1 6 a、基本鍵記憶部 1 6 b、鍵スペックテーブル 1 6 c、暗号化データ格納部 1 6 d が用いられる。基本鍵パラメータテーブル 1 6 a は基本鍵設定部 2 2 に用いられ、基本鍵記憶部 1 6 b、鍵スペックテーブル 1 6 c、暗号化データ格納部 1 6 d は暗号化処理部 2 7 及び復号化処理部 3 1 の両方に用いられる。

【0036】

なお、図 2 に示した各種のメモリ 2 6、2 8、3 0、3 2 は、レジスタ群であり、例えばデータ記憶装置 1 6 の所定のエリアに設けられる。

【0037】

このような構成において、データベースの暗号化を行う場合には、まず、オペレータの操作により基本鍵指定部 2 1 を通じて基本鍵を指定する。基本鍵設定部 2 2 は、この基本鍵指定部 2 1 によって指定された基本鍵のパラメータ値を基本鍵パラメータテーブル 1 6 a から読み出して基本鍵記憶部 1 6 b にセットする。

【0038】

具体的には、図 3 に示すような基本鍵設定ダイアログを通じて基本鍵の指定を行う。基本鍵設定ダイアログは、オペレータが基本鍵を任意に指定するための画面であり、その画面上に基本鍵指定ボタン部 4 1、OK ボタン 4 2、キャンセルボタン 4 3 が設けられている。基本鍵指定ボタン部 4 1 は複数のボタンからなり、オペレータがこれらのボタンの中の任意のボタンを押下すると、その押下したボタンの位置により基本鍵のパラメータ値が決定される。なお、OK ボタン 4 2 は基本鍵の指定を確定するためのボタン、キャンセルボタン 4 3 は基本鍵の指定を取り消すためのボタンである。

【0 0 3 9】

例えば、基本鍵指定ボタン部 4 1 に 1 6 個のボタン「1」～「1 6」が左から 4 個ずつ順に配列されているものとする。図 4 に示すように、基本鍵パラメータテーブル 1 6 a には、これらのボタンの位置に対応させて基本鍵のパラメータ値が定義されている。オペレータが基本鍵指定ボタン部 4 1 上の「1」のボタンを押下すると、この基本鍵パラメータテーブル 1 6 a に従って基本鍵のパラメータ値として「5」が決定される。同様に、基本鍵指定ボタン部 4 1 上の「2」のボタンを押下した場合には、基本鍵のパラメータ値として「7」が決定される。

【0 0 4 0】

次に、外部データベース記憶装置 1 8 にアクセスして、外部データベース記憶装置 1 8 に格納された各種データベースの中から暗号化対象となるデータベースを指定する。データベースの指定後、オペレータの操作により鍵スペック入力部 2 3 を通じて当該データベースの各データ項目に対する鍵スペックを指定する。鍵スペック設定部 2 4 は、この鍵スペック入力部 2 3 による鍵スペックの指定操作に従って鍵スペックテーブル 1 6 c に鍵スペック情報の登録を行う。

【0 0 4 1】

具体的には、図 5 に示すような鍵スペック設定ダイアログを通じて鍵スペックの指定を行う。鍵スペック設定ダイアログは、オペレータがデータベースの各列項目（フィールド）毎に暗号化方式（暗号化に用いる鍵の種類）を任意に指定するための画面であり、その画面上に暗号化方式指定欄 5 1、OK ボタン 5 2、キャンセルボタン 5 3 が設けられている。

【0042】

暗号化方式としては、各行毎に固有の鍵（行鍵）を用いた暗号化、各列毎に共通の鍵（列鍵）を用いた暗号化がある。ここでは、非暗号化を含め、0：非暗号化、1：行鍵、2：列鍵として、暗号化方式指定欄51にデータベースの各列項目に対する暗号化方式を数値入力するように構成されている。なお、OKボタン52は鍵スペックの指定を確定するためのボタン、キャンセルボタン53は鍵スペックの指定を取り消すためのボタンである。この鍵スペック設定ダイアログにて暗号化方式を指定すると、その指定内容が各列項目に対する鍵スペック情報として鍵スペックテーブル16cに登録される。

【0043】

図6に鍵スペックテーブル16cの登録例を示す。

【0044】

ここでは、データベースの列番号「1」の項目に対して非暗号化、列番号「2」の項目に対して行鍵、列番号「3」の項目に対して列鍵、列番号「4」の項目に対して列鍵、列番号「5」の項目に対して行鍵が登録されている。列番号「1」の項目は「code」、列番号「2」の項目は「name」、列番号「3」の項目は「state」、列番号「4」の項目は「age」、列番号「5」の項目は「phone」に相当する。

【0045】

このようにして、基本鍵記憶部16bに基本鍵が設定され、鍵スペックテーブル16cに各列項目に対する鍵スペック情報が設定されると、これらの設定情報を用いてデータベースの暗号化が以下のような手順で実行される。

【0046】

すなわち、図2に示すように、まず、外部データベース記憶装置18の中から指定されたデータベースがデータ読出し部25によって行単位（レコード単位）で読み出され、レコード入力メモリ26に順に格納される。暗号化処理部27はこのレコード入力メモリ26に格納されたレコードを基本鍵パラメータテーブル16a及び基本鍵記憶部16bを用いて暗号化する。このときの暗号化処理については後に図7を参照して詳しく説明する。

【0047】

暗号化処理部 2 7 にて暗号化されたレコードは暗号化レコード書込メモリ 2 8 に格納された後、データ書込み部 2 9 を通じて暗号化データ格納部 1 6 d に書き込まれる。このようにして、暗号化データ格納部 1 6 d 内に暗号化されたデータベースが作成される。

【0048】

一方、データベースの復号化は暗号化と逆の手順で行なわれる。

【0049】

すなわち、まず、暗号化データ格納部 1 6 d に格納された暗号化データベースが行単位（レコード単位）で読み出され、暗号化レコード読出メモリ 3 0 に順に格納される。復号化処理部 3 1 は、この暗号化レコード読出メモリ 3 0 に格納された暗号化レコードを鍵スペックテーブル 1 6 c 及び基本鍵記憶部 1 6 b を用いて復号化する。このときの復号化処理については後に図 7 を参照して詳しく説明する。復号化処理部 3 1 にて復号化されたレコードはレコード出力メモリ 3 2 に格納された後、データ出力部 3 3 を通じてデータファイル 3 4 に出力される。このようにして、データファイル 3 4 内に復号化されたデータベースが作成される。なお、データファイル 3 4 は図 1 のデータ記憶装置 1 6 の所定のエリアに設けられる。

【0050】

図 7 に具体例を示す。

【0051】

図 7 は本装置におけるデータベースの暗号化時と復号化時のデータの流れを示す図である。

【0052】

今、暗号化対象として指定されたデータベースの 1 行目のレコードがデータ読出し部 2 5 によって読み出され、レコード入力メモリ 2 6 に格納されたとする。この場合、図 1 1 (a) に示すデータベースを例にすると、そのデータベースの 1 行目の「1 0 0 1」, 「J h o n」, 「N e w Y o r k」, 「2 2」, 「4 0 7 - 2 2 8 - 6 6 1 1」といった 5 項目からなるデータが順にレコード入力メ

メモリ 26 に格納されることになる。

【0053】

暗号化処理部 27 は、この 5 項目のデータからなるレコードに対し、鍵スペックテーブル 16c を参照して各項目に応じた暗号化を行う。例えば、鍵スペックテーブル 16c に設定された内容が図 6 のような場合には、列番号「1」に相当する当該レコードの 1 項目（「code」）のデータについては暗号化せずに、そのまま暗号化レコード書込メモリ 28 に書き込む。

【0054】

また、列番号「2」に相当する当該レコードの 2 項目（「name」）のデータについては行鍵を用いて暗号化して暗号化レコード書込メモリ 28 に書き込む。行鍵は当該行番号と乱数によってランダムに生成されるものであり、各行毎に異なる値を有する。列番号「3」に相当する当該レコードの 3 項目（「state」）のデータについては列鍵を用いて暗号化する。この列鍵は各列に共通の値を有する。

【0055】

同様にして、列番号「4」に相当する当該レコードの 4 項目（「age」）のデータについては列鍵、列番号「5」に相当する当該レコードの 5 項目（「phone」）のデータについては行鍵を用いて、それぞれ暗号化して暗号化レコード書込メモリ 28 に書き込む。これにより、暗号化レコード書込メモリ 28 には、「1001」、「wjls」、「noevjolic」、「jh」、「jgdlttytfhDSk」といった 1 行分の暗号化データが生成されることになる。

【0056】

さらに、暗号化処理部 27 は、基本鍵記憶部 16b にセットされたパラメータ値を用いて各行に共通の基本鍵にて当該レコードの暗号化に用いた行鍵を暗号化することにより、その暗号化後の行鍵を暗号化レコード書込メモリ 28 に付加する。図 7 の例では、「9568」といったデータが暗号化後の行鍵である。

【0057】

以上のような処理がデータベースの各行に対して繰り返し行われ、暗号化後のデータベースが暗号化データ格納部 16d に格納される。この状態が図 11（b

)に相当する。

【0058】

一方、復号化時には、暗号化時と逆の処理になる。

【0059】

すなわち、暗号化データ格納部16dに格納された暗号化データベースが1レコード単位で暗号化レコード読出メモリ30に読み出される。今、1行目の暗号化レコードが暗号化レコード読出メモリ30に読み出されたとする。前記の例であれば、「1001」,「wjls」,「noevjolic」,「jh」,「jgdlt y t f h D S k」及び「9568」といった行鍵を含む6項目からなる暗号化データが順に暗号化レコード読出メモリ30に格納されることになる。

【0060】

復号化処理部31は、この6項目のデータからなるレコードに対し、鍵スペクタブル16cを参照して各項目に応じた復号化を行う。図6の例では、列番号「1」に相当する当該レコードの1項目（「code」）のデータについては非暗号化であるため、そのままレコード出力メモリ32に書き込む。

【0061】

また、列番号「2」に相当する当該レコードの2項目（「name」）のデータについては行鍵を用いて復号化してレコード出力メモリ32に書き込む。ただし、行鍵については暗号化時に基本鍵にて暗号化されているため、その基本鍵を用いて行鍵自体を復号化して元に戻す処理が必要となる。また、列番号「3」に相当する当該レコードの2項目（「name」）のデータについては列鍵を用いて復号化してレコード出力メモリ32に書き込む。

【0062】

同様にして、列番号「4」に相当する当該レコードの4項目（「age」）のデータについては列鍵、列番号「5」に相当する当該レコードの5項目（「phone」）のデータについては行鍵を用いて、それぞれ復号化してレコード出力メモリ32に書き込む。これにより、レコード出力メモリ32には、「1001」,「Jhon」,「New York」,「22」,「407-228-6611」といった1行分の復号化データ（元データ）が生成されることになる。

【 0 0 6 3 】

以上のような処理が暗号化データベースの各行に対して繰り返し行われ、復号化後のデータベースがデータファイル 3 4 に格納される。この状態が図 1 1 (c) に相当する。

【 0 0 6 4 】

以下、フローチャートを参照して本装置の動作について説明する。

【 0 0 6 5 】

ここでは、(a) データベースを暗号化する場合の処理と、(b) データベースを検索する場合の処理に分けて説明する。なお、このフローチャートで示す各機能を実現するプログラムは C P U が読み取り可能なプログラムコードの形態で前記プログラム記憶装置 1 4 の記録媒体に格納されている。また、このプログラムはプログラムコードの形態でネットワーク回線などの伝送媒体を介して伝送することもできる。

【 0 0 6 6 】

(a) データベースを暗号化する場合

図 8 は本装置にて実行されるデータベース暗号化処理の動作を示すフローチャートである。今、データベースが暗号化されていない状態で外部データベース記憶装置 1 8 に記憶されているものとする。この状態が図 1 1 (a) である。

【 0 0 6 7 】

データベースの暗号化を行う場合に、まず、図 8 (a) のフローチャートに示すように、基本鍵の設定を行う (ステップ A 1 1) 。この基本鍵の設定は、上述したように基本鍵設定ダイアログを通じて行う。

【 0 0 6 8 】

すなわち、図 8 (b) のフローチャートに示すように、データベースの暗号化時に図 3 に示すような基本鍵設定ダイアログが表示装置 1 2 に表示される (ステップ B 1 1) 。この基本鍵設定ダイアログには、基本鍵指定ボタン部 4 1 が設けられており、オペレータはその基本鍵指定ボタン部 4 1 に配列された複数のボタンの中の任意のボタンを押下することで基本鍵の指定を行う。

【 0 0 6 9 】

オペレータが基本鍵指定ボタン部 4 1 の中の任意のボタンを押下した後、OK ボタン 5 2 を押下して確定指示を行うと（ステップ B 1 2）、当該ボタンの位置に対応した基本鍵のパラメータ値が図 4 に示す基本鍵パラメータテーブル 1 6 a から読み出されて基本鍵記憶部 1 6 b にセットされる（ステップ B 1 3）。

【0 0 7 0】

次に、暗号化対象となるデータベースを指定する（ステップ A 1 2）。本実施形態では、本装置とは独立した外部データベース記憶装置 1 8 に各種のデータベース（元データ）を保持している。したがって、暗号化を行う場合には、データベース I / F 1 7 を介して外部データベース記憶装置 1 8 にアクセスし、その中から暗号化対象となるデータベースを指定するといった操作が必要となる。

【0 0 7 1】

暗号化対象となるデータベースを指定後、そのデータベースに設けられた各列項目の中で検索に利用する列項目と、暗号化を必要としない列項目をそれぞれ設定すると共に（ステップ A 1 3）、各列項目に対する暗号化鍵（行鍵と列鍵）を決定する（ステップ A 1 4）。

【0 0 7 2】

これらの設定は、上述した図 5 の鍵スペック設定ダイアログを通じて行う。この鍵スペック設定ダイアログは、オペレータがデータベースの各列項目（フィールド）毎に暗号化方式（暗号化に用いる鍵の種類）を任意に指定するための画面であり、前記ステップ A 1 2 にて、暗号化対象となるデータベースを指定した際に表示装置 1 2 に表示される。ここでは、非暗号化を含め、0：非暗号化、1：行鍵、2：列鍵として、前記図 5 の鍵スペック設定ダイアログに設けられた暗号化方式指定欄 5 1 にデータベースの各列項目に対する暗号化方式を数値入力するように構成されている。

【0 0 7 3】

この場合、図 1 1（a）に示すデータベースにおいて、検索に利用される列項目（つまり、高セキュリティが要求されない項目）は 3 列目の「state」と 4 列目の「age」であり、これらの列項目に対しては列鍵を指定し、その他の項目である 2 列目の「name」と 5 列目の「phone」は高セキュリティが

要求される項目として行鍵を指定するものとする。また、暗号化を必要としない列項目は1列目の「code」である。ここで設定された暗号化鍵は、鍵スペック情報として鍵スペックテーブル16cに図6のように登録される。

【0074】

このような設定操作の後、データベースの暗号化が以下のようにして実行される。

【0075】

すなわち、まず、データベースの各行のデータが第1行目から順に図2に示すレコード入力メモリ26に読み出される（ステップA15）。その際、鍵生成装置15の行鍵生成部15bによって当該行に割り付けられた行番号と乱数により行鍵がランダムに生成され、データ記憶装置16の所定のエリアに保持される（ステップA16）。

【0076】

ここで、レコード入力メモリ26に読み出された行データの各列項目が1列目から順次に指定され（ステップA17）、その指定された列項目に対する暗号化方式が鍵スペックテーブル16cに記憶された鍵スペック情報に基づいて判断され（ステップA18）、行鍵または列鍵を用いて暗号化される（ステップA19～A22）。

【0077】

具体的に説明すると、データベースの中の1列目の項目である「code」については図6の鍵スペックテーブル16cに示すように非暗号化項目として設定されているので、何もしない（ステップA18→A23）。つまり、「code」の項目は元データのままである。

【0078】

また、2列目の項目である「name」については行鍵が設定されているので、前記ステップA16にて生成された当該行番号に対応した行鍵（各行毎に固有の鍵）がデータ記憶装置16の所定エリアから読み出され（ステップA18→A21）、その行鍵にて2列目のデータが暗号化される（ステップA22）。

【0079】

また、3列目の項目である「state」については列鍵が設定されているので、当該列番号に対応した列鍵（各列毎に共通の鍵）が鍵生成装置 1 5 の列鍵生成部 1 5 c により生成され（ステップ A 1 8 → A 1 9）、その列鍵にて3列目のデータが暗号化される（ステップ A 2 0）。

【0080】

以下同様にして、4列目の項目である「age」については列鍵にて暗号化が行われ、5列目の項目である「phone」については行鍵にて暗号化が行われることになる。

【0081】

暗号化された各列項目のデータは、図 2 の暗号化レコード書込メモリ 2 8 に格納される。ここで、最終項目の暗号化が終了した時点で、当該行データの2列目及び3列目の項目の暗号化に用いられた行鍵が基本鍵にて暗号化されて暗号化レコード書込メモリ 2 8 に追加される（ステップ A 2 5）。この基本鍵は、鍵生成装置 1 5 の基本鍵生成部 1 5 a にて生成される。基本鍵生成部 1 5 a は、前記図 3 の基本鍵設定ダイアログにてオペレータが指定したパラメータ値を基本鍵記憶部 1 6 b から読み出し、そのパラメータ値に基づいて基本鍵を生成する。

【0082】

暗号化レコード書込メモリ 2 8 に1行分の暗号化データと、行鍵を基本鍵にて暗号化したデータが格納されると、それらのデータが暗号化データ格納部 1 6 d に保存される（ステップ A 2 5）。

【0083】

このような暗号化処理がデータベースの各行毎について繰り返し行なわれる（ステップ A 2 6 → A 1 5）。すべての行のデータの暗号化処理が終了し、最終的に得られた暗号化データベースの状態が図 1 1 （b）である。この暗号化データベースには、各行の最終項目に行鍵が基本鍵にて暗号化された状態で付加されている。

【0084】

（b）データベースを検索する場合

次に、暗号化後のデータベースを検索する処理について説明する。

【0085】

図9は本装置にて実行されるデータベース検索処理の動作を示すフローチャートである。今、前記(a)で説明した暗号化処理にて、データベースが暗号化されて暗号化データ格納部16dに保存されているものとする。

【0086】

まず、図9(a)のフローチャートに示すように、図示せぬデータベース検索用設定画面にて、検索情報の入力を行う(ステップC11)。検索情報の入力とは、検索対象となる列項目と、検索用の文字列(キーワード)を入力することである。これらの入力情報はデータ記憶装置16の所定のエリアに格納される。入力装置13を通じて検索情報が入力されると、検索前処理が実行される(ステップC12)。

【0087】

この検索前処理では、図9(b)のフローチャートに示すように、検索対象として入力された列項目が所定の列項目であるか否かが判断され(ステップD11)、所定の列項目であることが判明した場合には(ステップD11のYes)、その列項目に共通の列鍵で検索用の文字列が暗号化される(ステップD12)。

【0088】

所定の列項目とは、前記データベースの暗号化時に設定された検索対象項目(検索に利用される項目つまり高セキュリティが要求されない項目)であり、具体的には「state」,「age」の各項目が該当する。この検索対象項目には列鍵が設定されている。したがって、前記ステップD11では、鍵スペックテーブル16cを参照して当該列項目に設定された鍵の種類によって所定の列項目であるか否かの判断を行うことになる。所定の列項目であれば、鍵生成装置15の列鍵生成部15cにより当該列項目に対応した列鍵を生成し、その列鍵にて検索用の文字列を暗号化することになる。

【0089】

また、検索対象として入力された列項目が所定の列項目でなかった場合には(ステップD11のNo)、前記のような検索用文字列の暗号化は行われない。

【0090】

このような検索前処理の後、データベースの検索処理（図10参照）が行われ（ステップC13）、その検索結果として得られたデータが表示装置12に表示される（ステップC14）。図10にデータベースの検索処理を示す。

【0091】

図10は前記ステップC13の検索処理の動作を具体的に示すフローチャートである。

【0092】

まず、図10（a）のフローチャートに示すように、検索用文字列がデータベースとの比較文字列としてデータ記憶装置16の検索文字列格納部16eにセットされる（ステップE11）。この場合、上述したように検索対象として入力された列項目が所定の列項目（「state」, 「age」）であった場合には、前記検索前処理によって、当該検索用文字列がその列項目に対応した列鍵にて暗号化されて検索文字列格納部16eにセットされる。その他の列項目の場合には、暗号化されることなく、そのままの状態を検索文字列格納部16eにセットされる。

【0093】

次に、データ記憶装置16のデータベース格納エリア16aに格納された暗号化データベースの列番号による暗号化方式が判断される（ステップE12）。その結果、検索対象が列鍵で暗号化された所定の列項目に該当する場合には、その対象列の各行データが順次走査され（ステップE12→E13）、それらの行の暗号化文字列と前記検索文字列格納部16eにセットされた検索用文字列（暗号化された文字列）とが比較される（ステップE14）。

【0094】

この比較処理では、図10（b）のフローチャートに示すように、データベースから取り出された当該行の暗号化文字列と検索用の暗号化文字列とを比較して、両者が一致するか否かを判断する（ステップF11）。両者が一致した場合には（ステップF11のYes）、その一致した項目を含むレコードデータをデータベース検索結果として抽出する（ステップF12）。

【0095】

この処理を暗号化データベースの終端まで繰り返して、該当するデータを順次抽出し（ステップE15）、この抽出したデータを検索結果として出力する（ステップE21）。

【0096】

具体的に説明すると、図11（b）の暗号化データベースの例で、例えば「state」の項目の中の「Florida」といったデータを検索することが指定された場合には、まず、検索用データとして入力された「Florida」を「state」の3列目の列鍵で暗号化して「h*/fDD」を得る。この「h*/fDD」といったデータを「state」の列から検索する。これにより、コード番号の「1001」と「1008」に該当するデータが存在することがわかる。

【0097】

一方、検索対象が行鍵で暗号化された列項目つまり高セキュリティが要求される列項目に該当する場合には、その対象列の各行データが順次走査される（ステップE12→E16）。ここで、これらの行データの暗号化に用いられた各行鍵は基本鍵にて暗号化されているので、各行鍵を基本鍵にて復号化するといった処理が必要となる（ステップE17）。各行鍵が基本鍵にて復号化されると、それらの行鍵を用いて各行の暗号化文字列が復号化され（ステップE18）、その復号化の文字列と前記検索文字列格納部16eにセットされた検索用文字列（非暗号化文字列）とが比較される（ステップE19）。

【0098】

この比較処理では、図10（b）のフローチャートに示すように、データベースから取り出された当該行の復号化文字列と検索用の非暗号化文字列との比較により、両者が一致するか否かを判断する（ステップF11）。両者が一致した場合には（ステップF11のYes）、その一致した項目を含むレコードデータをデータベース検索結果として抽出する（ステップF12）。

【0099】

この処理を暗号化データベースの終端まで繰り返して、該当するデータを順次抽出し（ステップE20）、この抽出したデータを検索結果として出力する（ス

テップE21)。

【0100】

具体的に説明すると、図11(b)の暗号化データベースの例で、例えば「name」の項目の中の「John」といったデータを検索することが指定された場合には、まず、「name」の1行目に対応した行鍵「9654」(暗号化データ)を基本鍵にて復号化した後、その行鍵を用いて1行目の「wJIS」を復号化して「John」といったデータを得る。同様に、各行に対応した行鍵(暗号化データ)を基本鍵にて復号化した後、その行鍵を用いて各行目のデータを復号化して元のデータを得る。図11(c)に示すように「name」の項目の各行のデータを各行鍵にて復元した後、その中から検索用データとして入力された「John」と一致するデータを検索する。これにより、コード番号の「1001」に該当するデータが存在することがわかる。

【0101】

このように、データベースを暗号化する際に、検索に利用される所定の列項目については列共通鍵で暗号化することで、検索時には、検索用データをその列共通鍵で暗号化してデータベース上の暗号化データと比較して高速検索を実現できる。また、所定の列項目以外の列項目については各行毎に異なる鍵を与えて暗号化と、さらに、その行鍵を基本鍵にて暗号化しておくことで、鍵の解読を困難として高セキュリティ化を実現できるものである。

【0102】

(第2の実施形態)

前記第1の実施形態では、本発明を装置単体で構成したが、データベース管理を行う端末とデータベース検索を行う端末とに分けて、これらの端末でデータベースシステムを構築することも可能である。

【0103】

以下に、このようなデータベースシステムについて説明する。

【0104】

図12は本発明の第2の実施形態に係るデータベースシステムの構成を示すブロック図である。本システムは、1台のサーバ装置100と複数台(ここでは3

台のみ示す)の携帯端末200a, 200b, 200c…とで構成される。サーバ装置100と各携帯端末200a, 200b, 200c…との間はオフラインであり、データの授受は記録媒体400a, 400b, 400c…を通じて行われる。

【0105】

サーバ装置100は、データベースサービスを行うサーバコンピュータとして用いられるものであって、各端末に配布するデータの収集処理を行う配布データ収集装置101、データベースの暗号化処理を行う暗号化装置102、各種アプリケーションソフト(AP)を格納したAPソフト格納部103、各種のデータベースを格納したデータベース格納部104を備えている。APソフト格納部103及びデータベース格納部104は、例えば磁気ディスク装置等のデータ記憶装置によって構成される。この他、サーバ装置100には、特に図示しないが、汎用コンピュータに標準装備されている表示装置、入力装置等も設けられている。

【0106】

一方、携帯端末200a, 200b, 200c…は、サーバ装置100からデータベースの提供を受けるクライアントコンピュータとして用いられるものである。携帯端末200aは、暗号化されたデータベースを復号化処理する復号化装置201a、データベース検索処理を行うデータベース検索装置202aを備えている。携帯端末200b, 200cについても同様の構成であり、それぞれに復号化装置201b, 201c、データベース検索装置202b, 202cを備えている。また、携帯端末200a, 200b, 200cには、特に図示しないが、表示装置、入力装置等の他、媒体読込み装置も設けられている。これらの携帯端末200a, 200b, 200c…は、オンライン上でデータを閲覧するためのブラウザ機能を備えておらず、サーバ装置100との間のデータの授受はすべて記録媒体400a, 400b, 400c…を通じて行うように構成されている。

【0107】

記録媒体400a, 400b, 400c…は、例えばCFカード(コンパクト

フラッシュメモリカード) からなる可搬型の記録媒体である。カードリーダー/ライタ 300 は、これらの記録媒体 400 a, 400 b, 400 c … に対するデータの書込みや読出しを行うためのデバイスであり、サーバ装置 100 に接続されている。

【0108】

このような構成において、サーバ装置 100 側では、データベース格納部 104 内の各種データベースの中でオペレータが指定したデータベースを読み込み、暗号化装置 102 を通じて暗号化する。この場合、暗号化装置 102 では、前記第 1 の実施形態と同様の手法によりデータベースの暗号化する。すなわち、検索に利用される所定の列項目については列共通鍵で暗号化すると共に、所定の列項目以外の列項目については高セキュリティが要求される項目として、各行毎に異なる鍵を与えて暗号化し、さらに、その行鍵を基本鍵にて暗号化するという処理を行う。

【0109】

ここで、暗号化装置 102 によって暗号化されたデータベースをファイルに保存し、この暗号化ファイルを例えば CF カード等の可搬型記録媒体 400 a, 400 b, 400 c … にカードリーダー/ライタ 300 を用いて格納する。この場合、記録媒体 400 a, 400 b, 400 c … に暗号化ファイルを格納する際に、図 13 に示すように、暗号化データファイル 402 の他に、鍵スペックテーブル 403、基本鍵パラメータテーブル 404、さらにアプリケーションプログラム 401 も格納しておく。

【0110】

鍵スペックテーブル 403 は、データベースの各列 (フィールド) 毎に定義された暗号化方式の種類 (非暗号化, 行鍵, 列鍵) を記憶したテーブルであり、前記第 1 の実施形態における鍵スペックテーブル 16 c と同様の構成を有する (図 6 参照)。基本鍵パラメータテーブル 404 は、基本鍵のパラメータ値が登録されたテーブルであり、前記第 1 の実施形態における基本鍵パラメータテーブル 16 a と同様の構成を有する (図 4 参照)。この鍵スペックテーブル 403 及び基本鍵パラメータテーブル 404 は、暗号化装置 102 内に保持されていたもので

ある。また、アプリケーションプログラム401は、データベース検索用のプログラムであり、APソフト格納部103内に保持されていたものである。

【0111】

これらの情報が格納された記録媒体400a, 400b, 400c…は、携帯端末200a, 200b, 200c…を扱う各ユーザにそれぞれ配布される。各ユーザは、配布された記録媒体400a, 400b, 400c…を自身が持つ端末に挿入することで、データ検索を行うことができる。

【0112】

すなわち、例えば携帯端末200aであれば、配布された記録媒体400aを挿入することで、その記録媒体400aに記録されていたデータ検索用のアプリケーションプログラム401、暗号化データファイル402の他に、鍵スペックテーブル403、基本鍵パラメータテーブル404を読み込む。そして、データ検索用のアプリケーションプログラム401を起動し、所望の列項目を指定して、暗号化データファイル402に対するデータ検索を行い、その検索結果として得られたデータを復号化して表示する。

【0113】

データ検索は、携帯端末200aに設けられたデータベース検索装置202aにて行われる。このデータベース検索装置202aは、データ検索用のアプリケーションプログラム401に従って動作し、前記第1の実施形態と同様のデータベース検索処理を実行する。また、データの復号化は、復号化装置201aにて行われる。この復号化装置201aは、鍵スペックテーブル403及び基本鍵パラメータテーブル404を参照して、前記第1の実施形態と同様のデータベース復号化処理を実行する。

【0114】

このように、データベース管理を行う端末とデータベース検索を行う端末とに分けてデータベースシステムを構築するようにすれば、例えば顧客管理用のデータベースを暗号化して記録媒体に記録し、これを営業マンに配布し、営業マンは別の端末を用いてデータ検索を行うといったような利用が可能となる。この場合、記録媒体に記録されたデータベースは上述したような手法にて暗号化されてい

るため、そのデータの機密性を保持することができる。また、記録媒体には、暗号化ファイルだけでなく、データ検索用のアプリケーションプログラムも格納されている。したがって、携帯端末側にはデータ検索用のアプリケーションプログラムを搭載しておく必要はなく、簡易な構成の携帯端末で本システムを実現できるといった利点がある。

【0115】

【発明の効果】

以上詳記したように本発明によれば、データベースを暗号化する際に、検索に利用される所定の列項目以外の列項目のデータについては、各行毎に鍵を異ならせて暗号化し、さらに、当該列項目の暗号化に用いられた鍵を別の鍵で再暗号化するようにしたため、鍵の解読を困難として高セキュリティ化を実現することができる。

【図面の簡単な説明】

【図1】

本発明の第1の実施形態に係るデータベース管理装置の構成を示す図。

【図2】

前記データベース管理装置の構成を機能的に示したブロック図。

【図3】

前記データベース管理装置における基本鍵設定ダイアログの構成を示す図。

【図4】

前記データベース管理装置における基本鍵パラメータテーブルの一例を示す図。

【図5】

前記データベース管理装置における鍵スペック設定ダイアログの構成を示す図。

【図6】

前記データベース管理装置における鍵スペックテーブルの登録例を示す図。

【図7】

前記データベース管理装置におけるデータベースの暗号化時と復号化時のデー

タの流れを示す図。

【図 8】

前記データベース管理装置にて実行されるデータベース暗号化処理の動作を示すフローチャート。

【図 9】

前記データベース管理装置にて実行されるデータベース検索処理の動作を示すフローチャート。

【図 1 0】

前記図 9 のステップ C 1 3 の検索処理の動作を具体的に示すフローチャート。

【図 1 1】

前記データベース管理装置におけるデータベースの構成を説明するための図であり、図 1 1 (a) は暗号化前の状態、同図 (b) は暗号化後の状態、同図 (c) は復号化後の状態を示す図。

【図 1 2】

本発明の第 2 の実施形態に係るデータベースシステムの構成を示すブロック図。

【図 1 3】

前記データベースシステムに用いられる記録媒体のデータ内容を示す図。

【符号の説明】

1 1 … C P U

1 2 … 表示装置

1 3 … 入力装置

1 4 … プログラム記憶装置

1 5 … 鍵生成装置

1 5 a … 基本鍵生成部

1 5 b … 行鍵生成部

1 5 c … 列鍵生成部

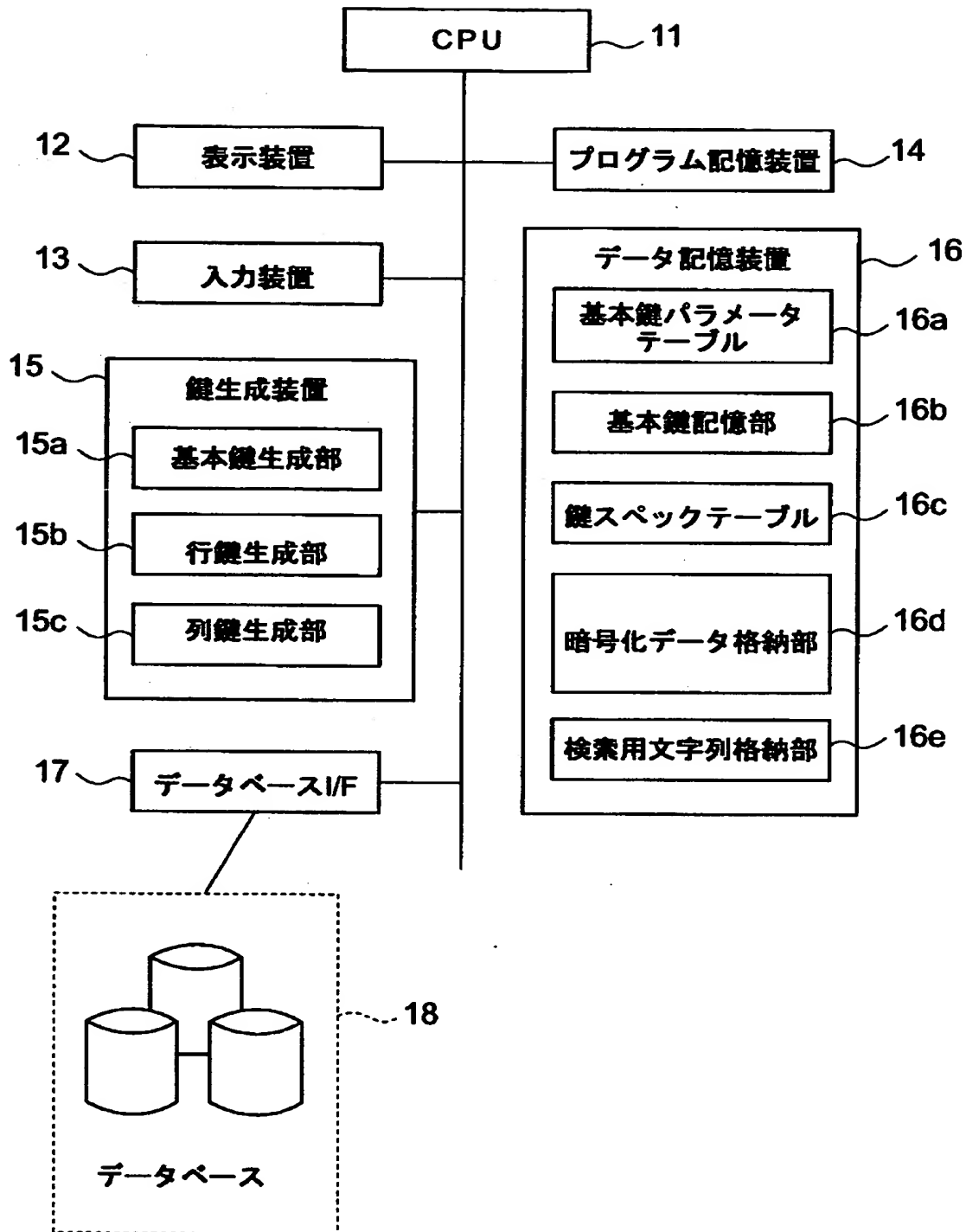
1 6 … データ記憶装置

1 6 a … 基本鍵パラメータテーブル

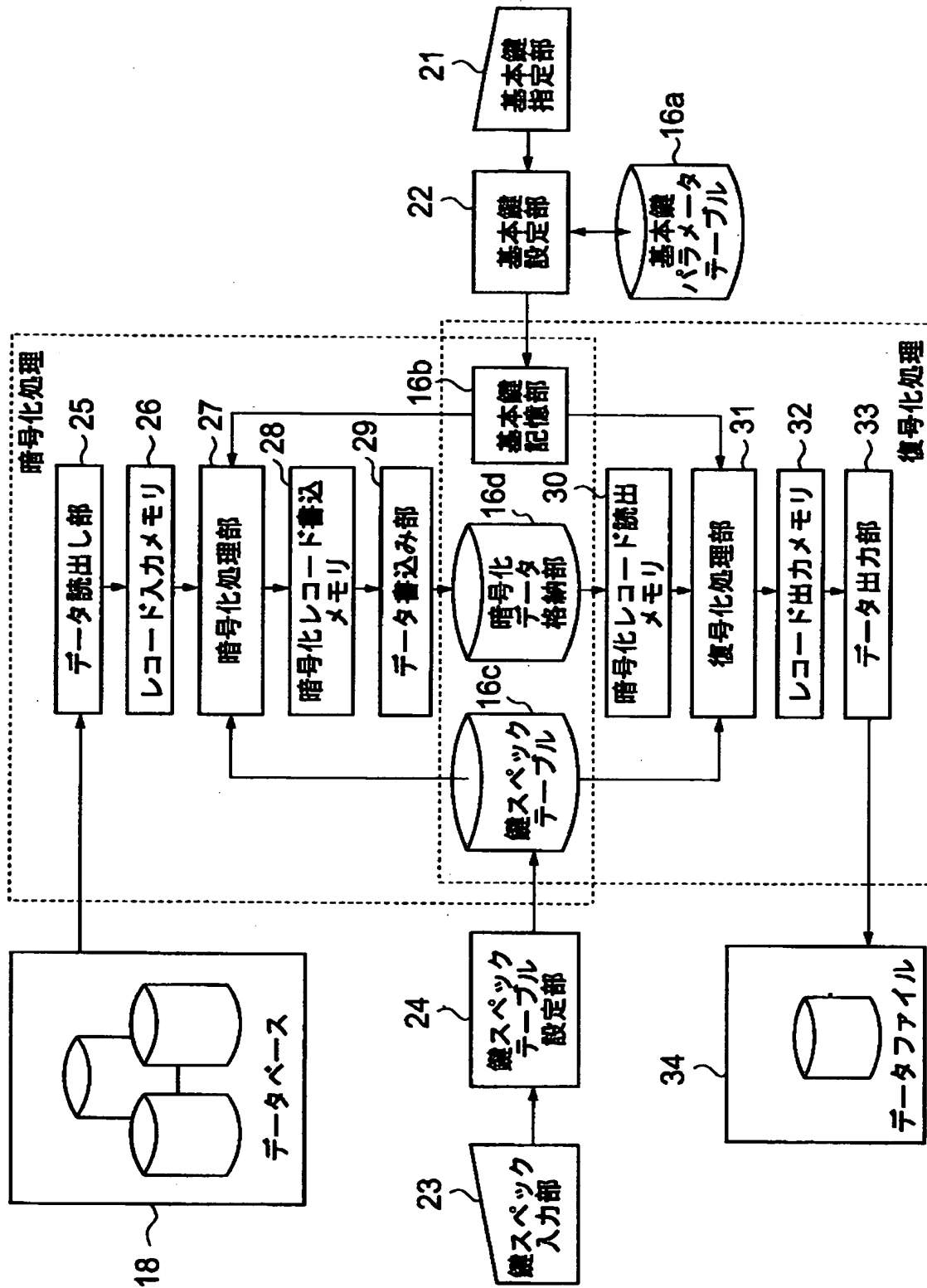
- 16b…基本鍵記憶部
- 16c…鍵スペックテーブル
- 16d…暗号化データ格納部
- 16e…検索文字列格納部
- 17…データベース I/F
- 18…外部データベース記憶装置
- 100…サーバ装置
- 200a～200c…携帯端末
- 300…カードリーダー/ライター
- 400a～400c…記録媒体

【書類名】 図面

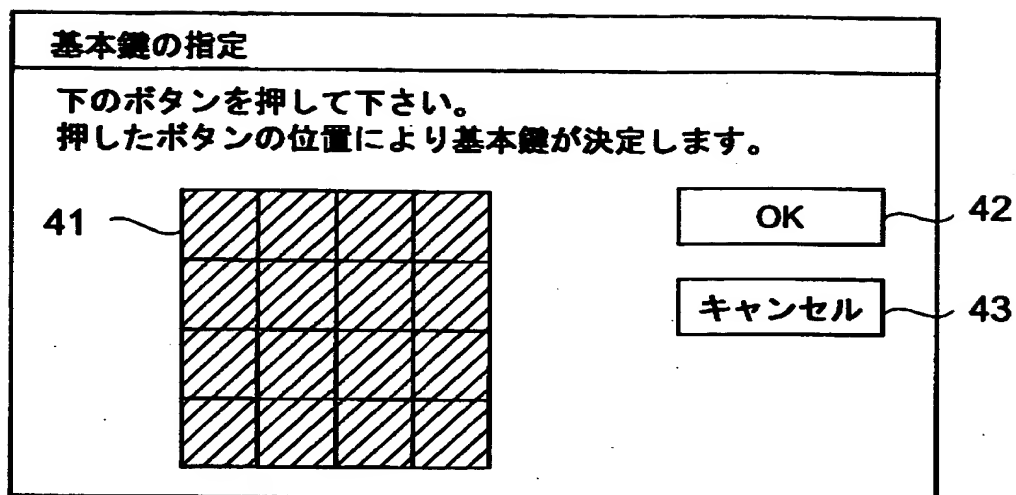
【図 1】



【図 2】



【図 3】



【図 4】

基本鍵パラメータテーブル 16a

ボタン位置	パラメータ値
1	5
2	7
3	9
4	11
5	13
6	15
7	17
8	19
9	21
10	23
11	25
12	27
13	29
14	31
15	33
16	35

【図 5】

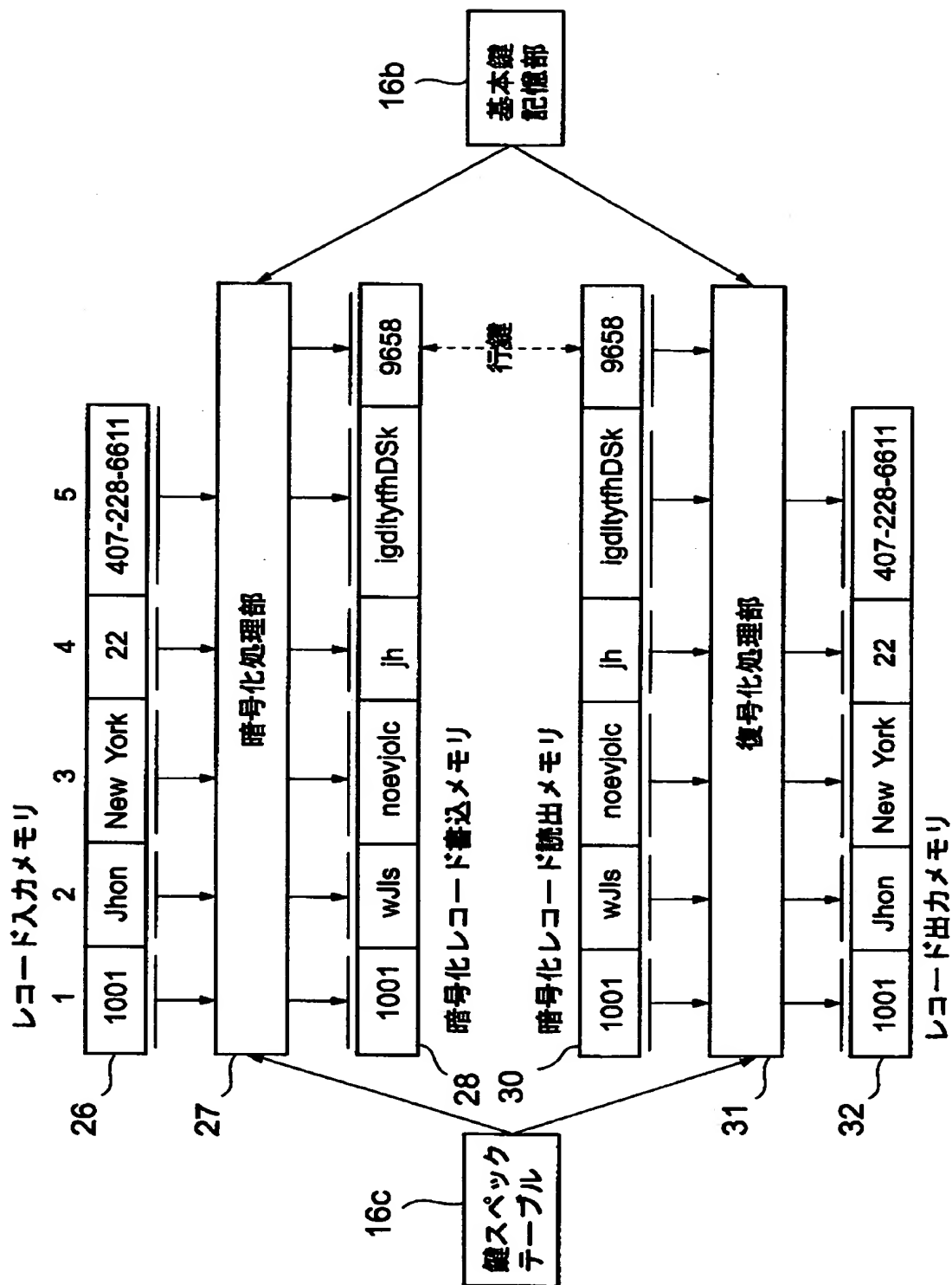
鍵スペックの指定			
各列項目に暗号化方式を指定して下さい。 0: 非暗号化 1: 行鍵 2: 列鍵			
51	列番号	暗号化鍵	OK 52
	1	0	
	2	行鍵	キャンセル 53
	3	列鍵	
	4	列鍵	
	5	行鍵	
	⋮	⋮	
	n		

【図 6】

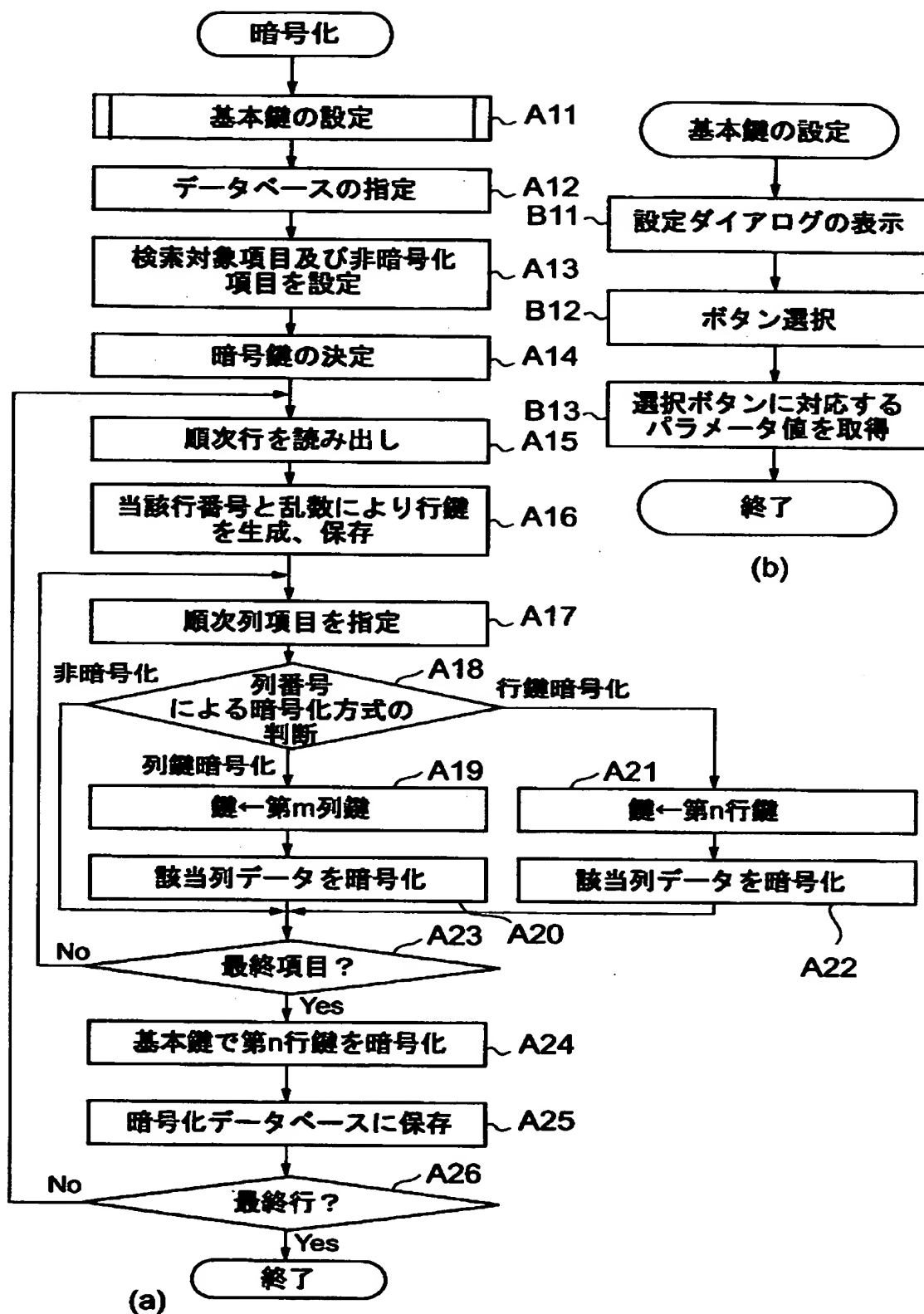
鍵スペックテーブル 16c

列名前	列番号	暗号化鍵
(code)	1	0
(name)	2	行鍵
(state)	3	列鍵
(age)	4	列鍵
(phone)	5	行鍵

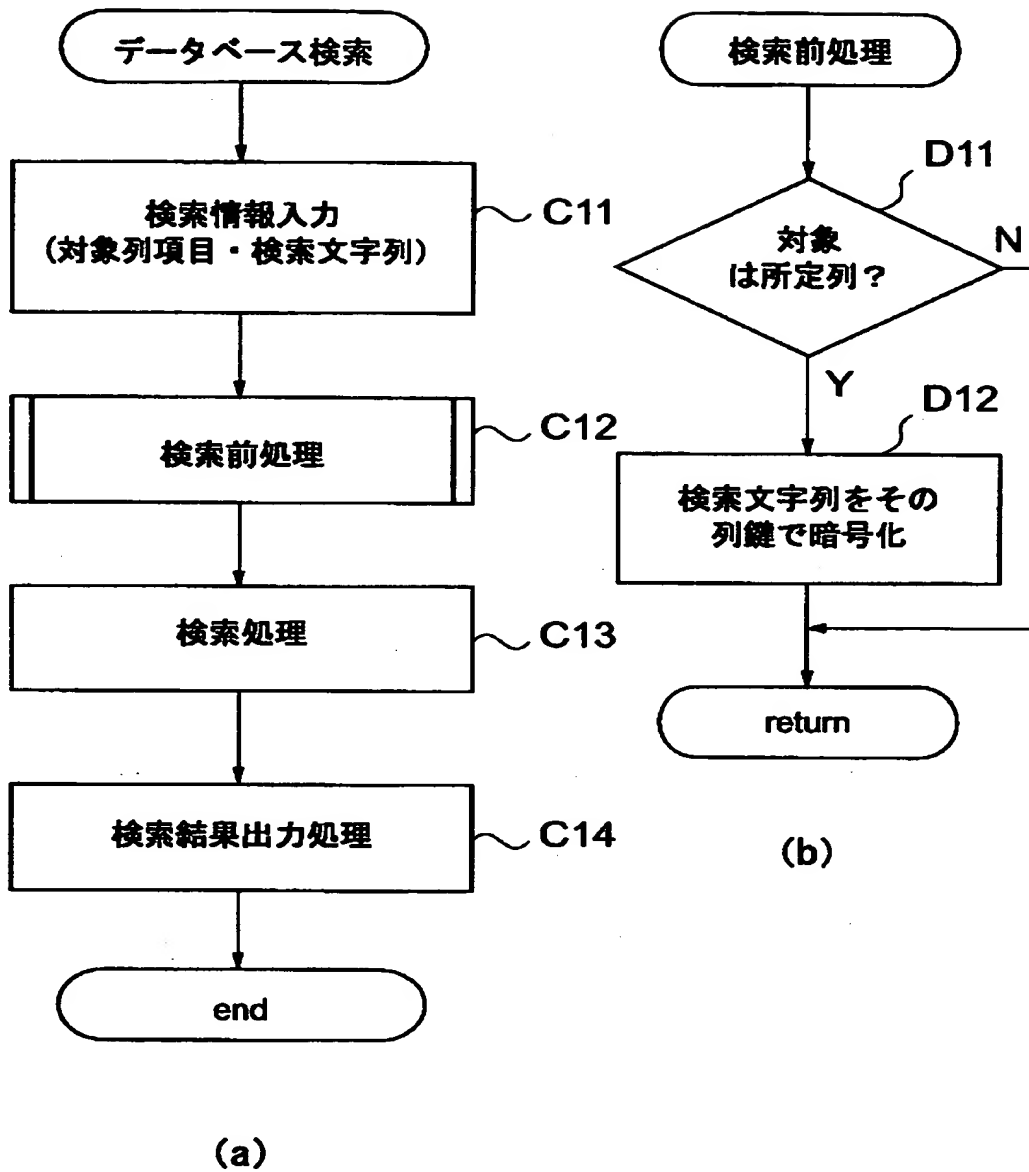
【図 7】



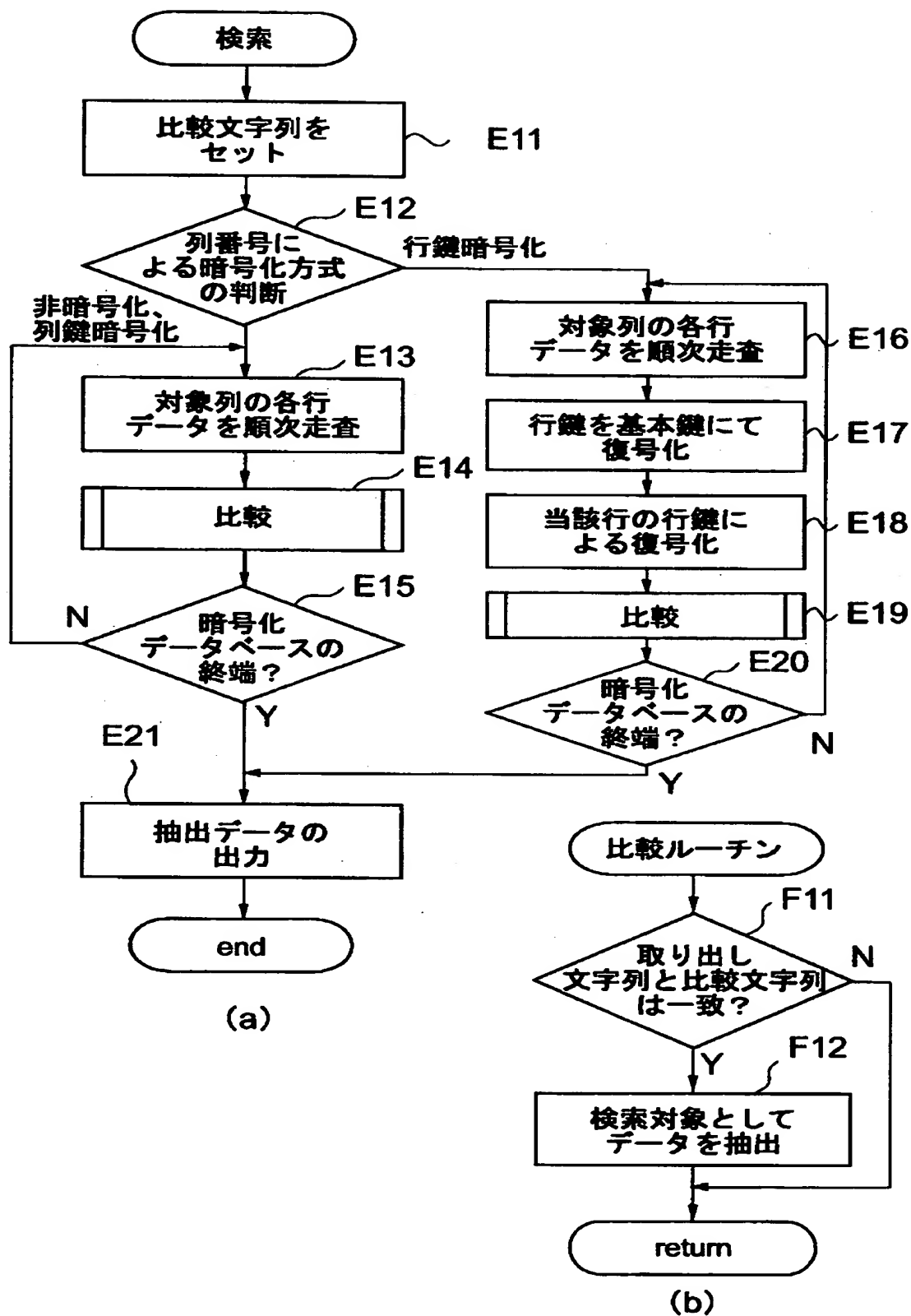
【図 8】



【図 9】



【図 10】



【図 1 1】

(a)

code	name	state	age	phone
1001	Jhon	New York	22	407-228-6611
1002	Chris	Florida	21	123-456-7890
1003	Michael	Minnesota	27	101-202-3030
1004	David	Iowa	34	523-761-0045
1005	Mark	New York	30	832-962-9001
1006	Daniel	Iowa	25	231-981-9454
1007	George	Idaho	31	561-545-4389
1008	Henry	Florida	22	239-203-9800
1009	Joe	New Jersey	27	239-129-9898

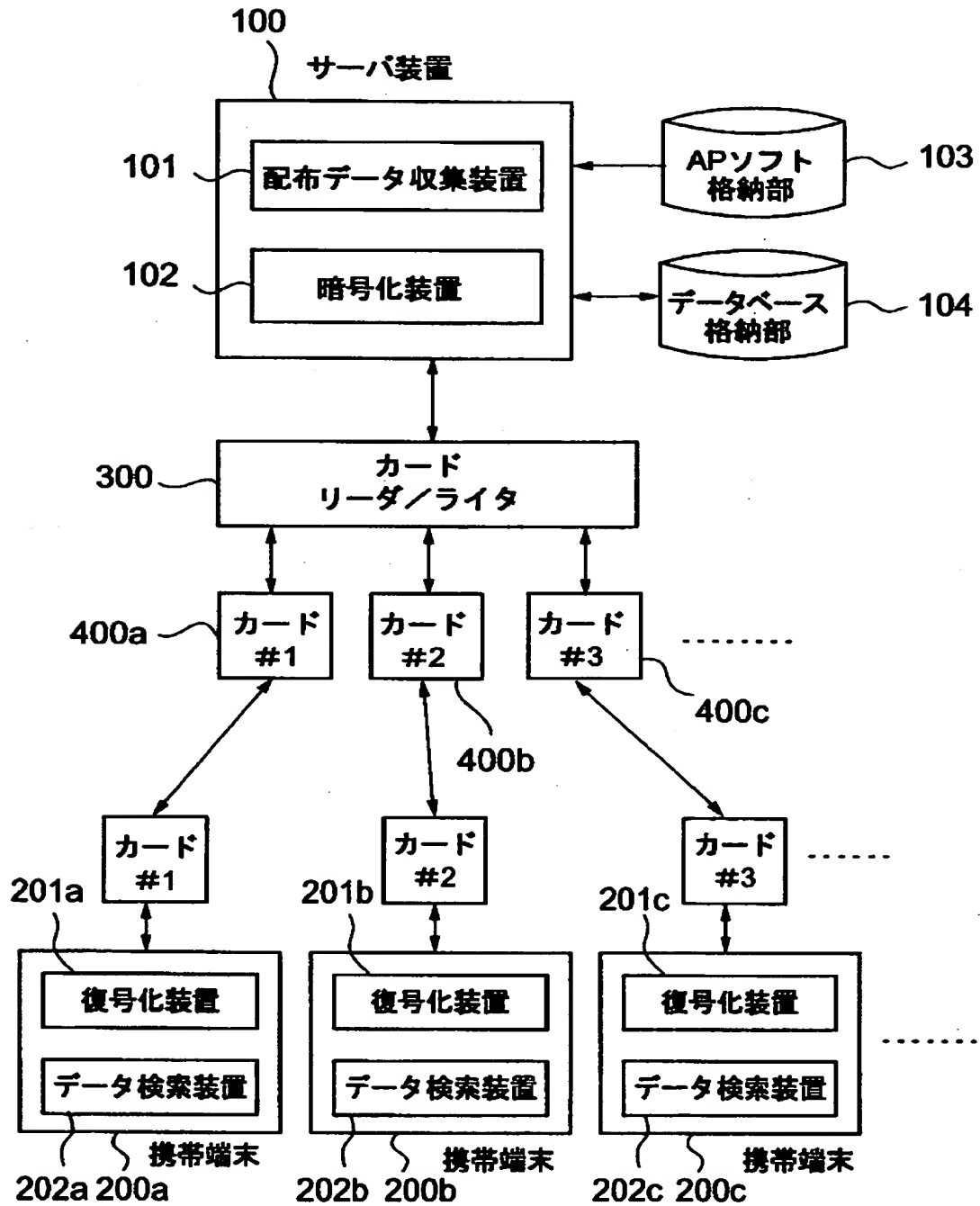
暗号化 ↓ 列鍵行鍵

code	name	state	age	phone	line key
1001	wJls	noevjolc	jh	igdltyrfhDSk	9658
1002	ddGGa	h*/fDD	hg	LKtYfDSkoKow	9143
1003	1jkl+P	gah{6xpVd	tY	hkliydageQk	8278
1004	3eK@s	KHHS	Kl	d+fDIKnBrUf	4358
1005	erlN	noevjolc	Gv	wsdERfvW2Sdf	5784
1006	F>sSlu	KHHS	ij	1xcVImFmkjpo	9743
1007	{:ld?k	IJHFD	LK	kjwDkJGvfDoa	3935
1008	rhJKd	h*/fDD	jh	e419h-ka+qwh	7412
1009	ifd	ASoChijlO-	tY	qLFUjCVkj@kl	9593

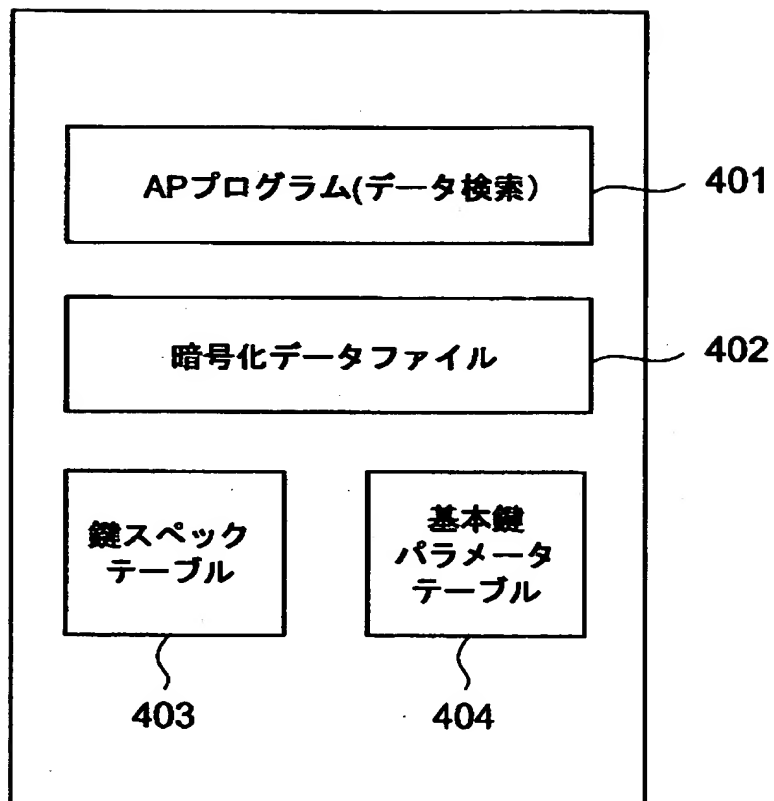
復号化 ↓ 列鍵行鍵

code	name	state	age	phone
1001	Jhon	New York	22	407-228-6611
1002	Chris	Florida	21	123-456-7890
1003	Michael	Minnesota	27	101-202-3030
1004	David	Iowa	34	523-761-0045
1005	Mark	New York	30	832-962-9001
1006	Daniel	Iowa	25	231-981-9454
1007	George	Idaho	31	561-545-4389
1008	Henry	Florida	22	239-203-9800
1009	Joe	New Jersey	27	239-129-9898

【図 1 2】



【図 1 3】



【書類名】 要約書

【要約】

【課題】 データベース上の特定のデータ項目に対するセキュリティを他のデータ項目よりも高めて暗号化する。

【解決手段】 外部データベース記憶装置 18 に記憶されたデータベースをデータベース I/F 17 を介して読み込む。ここで、鍵スパックテーブル 16 c を参照してデータベースの所定の列項目のデータについて当該列項目に共通の列鍵を用いて暗号化し、その他の列項目のデータについては高セキュリティが要求される項目として各行毎に固有の行鍵を用いて暗号化する。さらに、基本鍵記憶部 16 b を参照して前記行鍵を基本鍵にて暗号化し、前記暗号化されたデータベースと共に暗号化データ格納部 16 d に格納する。このように、各行毎に鍵を異ならせて暗号化し、さらに、当該列項目の暗号化に用いられた鍵を別の鍵で再暗号化することで、鍵の解読を困難として高セキュリティ化を実現することができる。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000001443]

1. 変更年月日 1998年 1月 9日

[変更理由] 住所変更

住 所 東京都渋谷区本町1丁目6番2号
氏 名 カシオ計算機株式会社